Technical Overview of Fissile Material Transparency Technology Demonstration

Executive Summary

There are two major objectives for the Fissile Material Transparency Technology Demonstration (FMTTD). The first is to demonstrate to the Russian delegation that a six-attribute measurement system with information barrier (AMS/IB) can be built with sufficient protection to allow measurement of classified components without revealing classified information. The second is to construct this AMS/IB in such a manner as to convince the Russian delegation that it would be possible for a monitoring party to fully authenticate operation of the system.

Six attributes will be measured in the demonstration AMS/IB. These are:

(1) plutonium isotopic ratio,
(2) plutonium mass,
(3) absence of oxide,
(4) presence of plutonium,
(5) symmetry of the plutonium, and
(6) plutonium age.

To measure these attributes, the demonstration AMS/IB will use three detection systems (Fig. 1) connected to four analyzing computers.

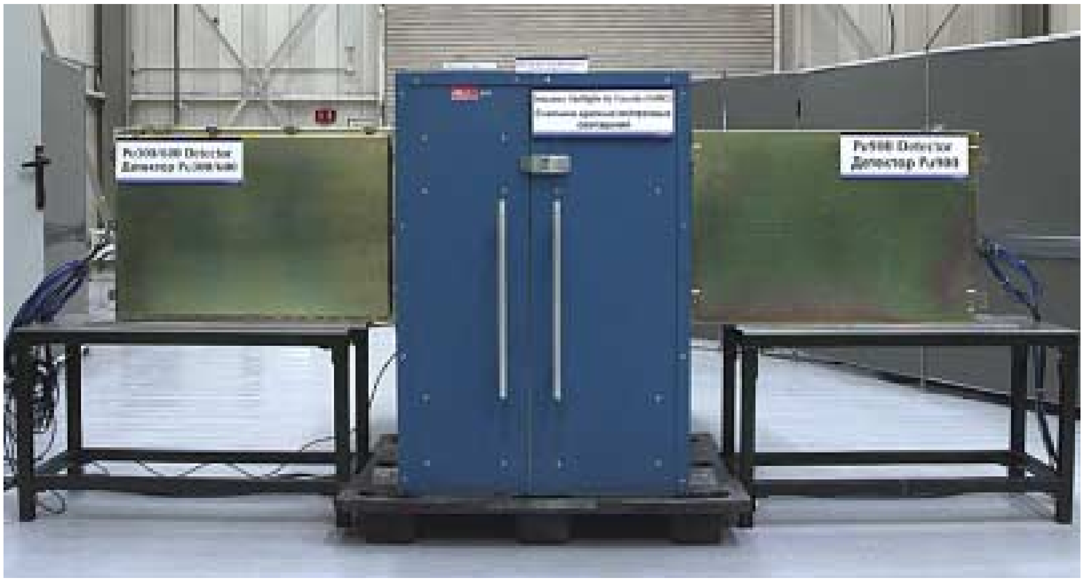

Fig. 1. The three AMS/IB detectors. On the left is the Pu300/600, a medium-sized (50%), germanium-detector based, high-resolution gamma-spectroscopy (HRGS) system. In the center is a neutron multiplicity counter (NMC), with the ability to individually read out each bank of tubes. On the right is the Pu900 , a larger (66%), germanium-detector-based HRGS system.

The medium-sized HRGS detector (Fig. 2) and associated analyzer will be used to measure Pu presence, isotopic ratio, and Pu age. The larger HRGS detector and associated analyzer will be used to (1) measure oxygen content, and (2) identify the presence of oxides.

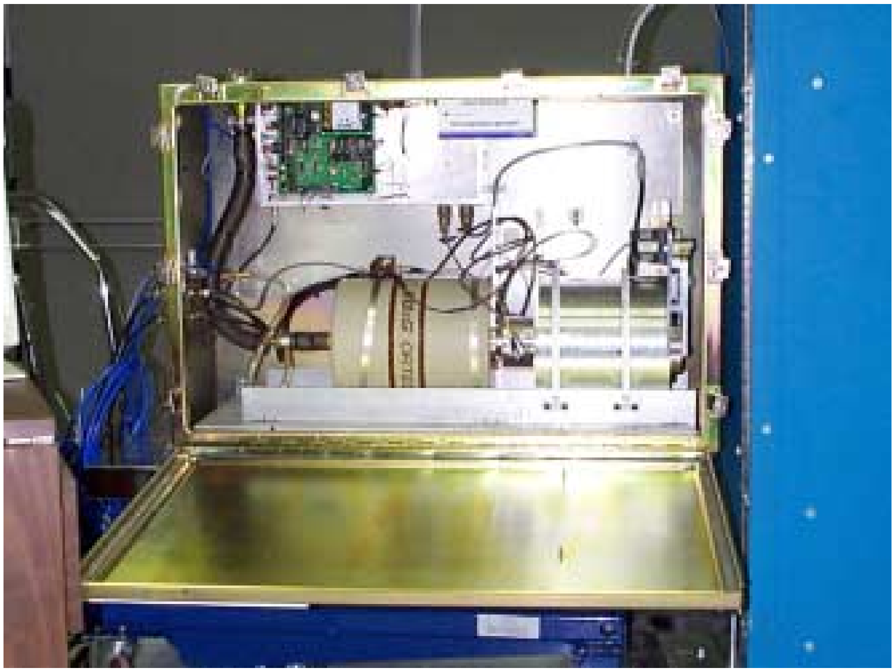

Fig. 2. Interior view of the medium-sized HRGS Pu300/600 detector.

The neutron multiplicity counter (Fig. 3) and NMC analyzer will be used to identify the presence of oxides and, in conjunction with the medium-sized HRGS detector, to determine Pu mass. Only if an oxide signature is detected in both the HRGS and the NMC will an object be determined to contain oxide. Finally, the signals from eight segments of the multiplicity counter will be used to measure the symmetry of the object being monitored.

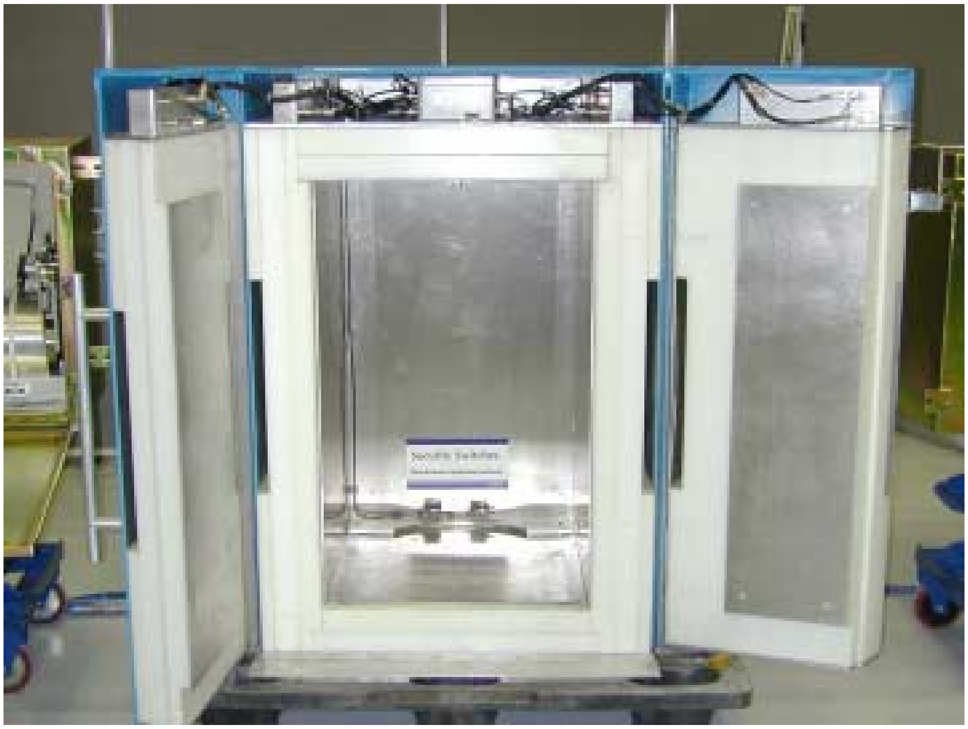

Fig. 3. The NMC open, showing the security switches that detect whether a container is designed to contain classified or unclassified items.

When the AMS/IB is used in secure mode to measure the attributes of a nuclear weapon component, classified data are produced within the system, but these data are protected from outside access by the information barrier. Only unclassified yes/no results for the six attributes examined are shown on the AMS/IB display panel. The demonstration AMS/IB can operate with the doors to the shielded electronics rack either open or closed. When the access doors are closed, a red and green light-emitting diode (LED) display is the only possible output from the system (Fig. 4).

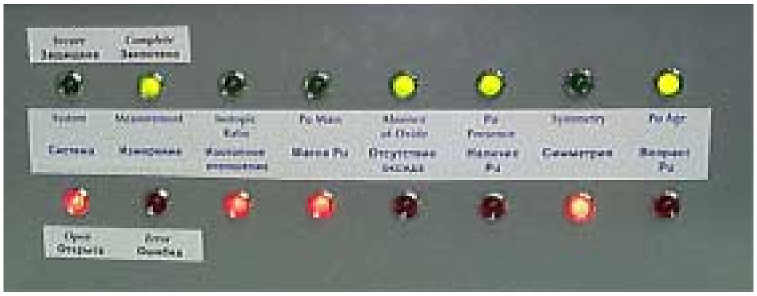

Fig. 4. Unclassified output of the AMS/IB display.

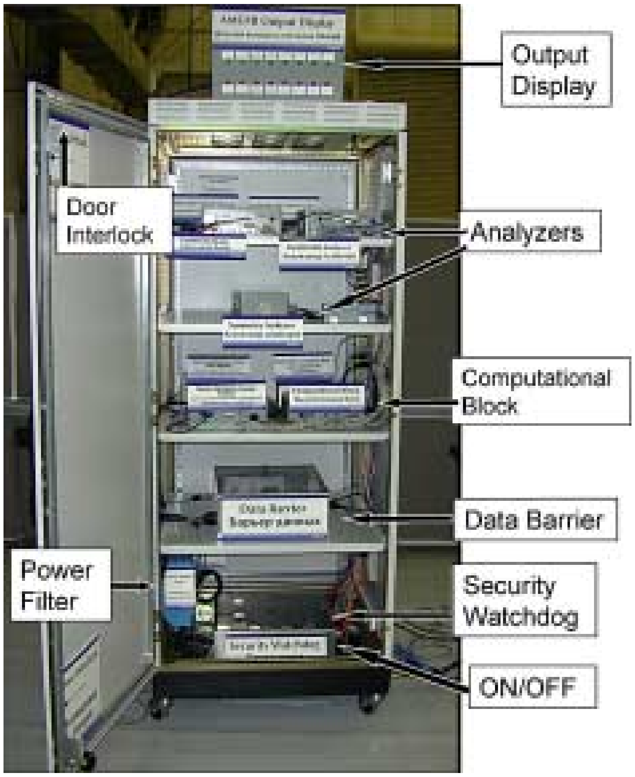

Fig. 5. Shielded electronics rack.

In this configuration, either classified items or unclassified reference materials can be measured, but only the simple unclassified display is possible, and if the access door is opened, all power is immediately removed from the system. Since no classified data are stored except in volatile memory, which is lost when power is removed, this power removal ensures that no classified information can remain in the AMS/IB after the door is opened. If, and only if, a specially modified container for use with unclassified materials is present in the NMC, will the security watchdog restore power to the AMS/IB following a delay of approximately 20 seconds. This will allow authentication measurements to take place using known unclassified authentication materials. If the modified container is removed from the AMS/IB while the door is open, all power to the system will be immediately cut off and will remain off until the modified container is replaced or the access door is closed.

Raw data generated in any of the three detectors pass into the shielded electronics rack (Fig. 5) and to one of the four data acquisition systems and analyzers.

The analyzed results pass into the computational block where the attribute threshold values are stored and threshold comparisons are performed. The outputs from the computational block, in the form of pass/fail results, leave the shielded enclosure through the data barrier and are sent to the unclassified display. Although the outputs from the computational block are unclassified, these signals are inside the shielded enclosure and are treated as possibly classified until they pass out of the enclosure through the data barrier, which ensures that they are unclassified.

There are several additional important elements of the AMS/IB that are not in the direct data-processing path described above. All power for the AMS/IB enters the security watchdog through an AC line filter. The only function of the security watchdog is to monitor the security status of the entire system and to remove all power from all other AMS/IB elements if any of the access doors are opened or if classified material is introduced into the system incorrectly. The security mode of the security watchdog (and hence the entire AMS/IB) is set by the security switches that are depressed by the security container itself without human intervention. In addition, several data-control switches are used to start a background run, start calibration runs, and start measurement runs.

The AMS/IB for the FMTTD uses five computers; one each for the two HRGS systems, two for the neutron multiplicity counter (one for mass and oxides, and one for symmetry), and one for the computational block. All five computers employ simple hardware (PC/104-specification computers) and simple software. Most importantly, all of these computers are located within the shielded enclosure. All communications with the unclassified area are either through simple hardware switch controls (the data-control switches) or filtered through the (hardware) data barrier. There is at least one “hardware only” element between each of these CPUs and the outside world. Thus, the programming in the CPUs cannot affect the hardware components of the information barrier. In particular, it is physically impossible for one of the CPUs to reprogram either the data barrier or the display to reveal classified information. In addition, all data flow within the AMS/IB is unidirectional: no information can be passed from the display back to the remainder of the system or from the computational block to the detectors.

Another important feature of the demonstration AMS/IB is the separation between the security switches and the data-control switches. The security switches control the security watchdog directly. The security watchdog, in turn, controls the power to all of the other elements of the AMS/IB, but there is no other connection from the security watchdog to the CPUs. Thus, the CPUs do not know the position of the security switch and have no way of knowing whether they are processing classified or unclassified data. This adds some assurance that the analyzers are operating similarly whether or not a classified item is being measured.

1.0 INTRODUCTION

The objective of this report is to provide an overview of the Fissile Material Transparency Technology Demonstration (FMTTD).

One of the challenges for a number of future monitoring regimes will be to perform measurements of nuclear weapon components without obtaining access to or revealing classified information. The first part of this challenge—measuring nuclear weapon components—is relatively straightforward. Although it presents some technical difficulties, proven methods exist, and their technical feasibility has been established in both the US and the Russian Federation.

A second part of the challenge—making such measurements without divulging classified information—is less straightforward in a monitoring setting, where a monitoring party who should not have access to information considered classified by the host would observe or participate in the measurements. Especially with such a monitoring party present, steps must be taken to guarantee prevention of the release of classified information, and for legal and security reasons extremely high standards of protection must be applied.

A third part of the challenge is the necessity to permit the monitoring party to authenticate the measurements, i.e., to establish that the measurements are accurate.

The purpose of the FMTTD is to demonstrate that these challenges can be met. To this end, the FMTTD has the following three immediate goals:

(1) demonstrate a system design capable of making the necessary measurements accurately and authentically in a short time and at a reasonable cost;
(2) demonstrate that classified information can be protected if necessary precautions are taken; and
(3) demonstrate how such a measurement system can be authenticated.

The demonstration is intended to be a “proof of concept.” It shows one way in which the challenge can be met, but it is only a first step. The concept will require further development and refinement, as well as adaptation to specific conditions, before it can be implemented.

It is anticipated that several distinct cooperative efforts would result from this demonstration. Hence, an additional key goal of the demonstration is to begin cooperative development, in which different US and Russian Federation subgroups could begin working together on the next steps for several possible specific applications. In this way, when the time comes to implement such systems, sound technical solutions that will meet the requirements of both countries will be ready.

2.0 US-RUSSIAN COOPERATION ON TRANSPARENCY TECHNOLOGY

As the two leading nuclear nations, the United States and the Russian Federation have not only a common interest in nuclear security and stability but also a special responsibility to continue their efforts to promote global security and stability. In recent years, the United States and the Russian Federation have undertaken a number of cooperative initiatives in this direction. Examples include:

- START I and START II to reduce accountable nuclear weapons launchers
- the highly enriched uranium/low-enriched uranium (HEU/LEU) agreement, whereby the US purchases from the Russian Federation LEU derived from weapons HEU;
- the Trilateral (US-RF-IAEA) initiative to apply bilateral and IAEA inspections to nuclear materials no longer needed for weapons purposes;
- the Plutonium Production Reactor Agreement, which assists in the cessation of plutonium production for weapons purposes and monitors Pu produced in the interim; and
- the Fissile Material Storage Facility, which is designed to safely and securely store fissile material from nuclear weapons.

As part of this process, the two countries rely on mutually agreed methods, sometimes referred to as “transparency measures,” to provide confidence that the objectives and conditions underpinning these initiatives are being satisfied.

Through joint work, significant progress has been made in the development and implementation of mutually acceptable transparency arrangements. As technology has progressed and as experience has been gained, the transparency measures have become increasingly sophisticated and effective. Transparency measures are now being used routinely in applications that, in the past, would have been regarded as too sensitive for any form of bilateral or international interaction.

The cooperation in construction of the FMSF and other agreements in existence or under construction have brought focus on sensitive subjects closely related to nuclear weapons materials and weapons technologies. Consequently, there will be an increasing need for transparency methods that can be used in these sensitive applications without disclosing sensitive or classified information. Such methods pose significant challenges, not only for technical reasons, but also because both countries have very strict requirements for protecting classified information.

Based on past experience, the optimal approach to overcoming these challenges is cooperative work. By combining the best of Russian and American technologies and ideas, practical solutions can be developed that are well-adapted to the requirements and conditions in each country. A major goal of the Fissile Material Transparency Technology Demonstration is to pave the way for further technical cooperation in this area.

3.0 INFORMATION BARRIERS

An information barrier is a combination of technology and procedures designed to protect classified information from dissemination while permitting the transmission of certain agreed-upon, unclassified information.

At the same time, the information barrier must also enable the monitoring party to authenticate the accuracy of the information. These two goals are often competing.

In this demonstration, the information barrier is a specific set of equipment, with accompanying procedures, known as the "Attribute Measurement System with Information Barrier" or AMS/IB.

As illustrated in Fig. 6, an AMS/IB can be thought of as a box (the IB) with the measuring and computational systems on the protected side (inside) and the display on the open side (outside). All classified data generated by the measurement system will remain inside the box.

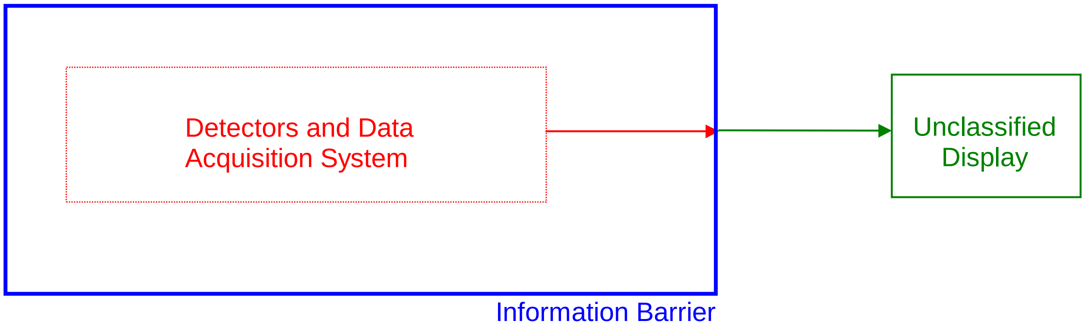

Fig. 6. Conceptual AMS/IB system for the protection of classified information. Everything inside the IB "box" is protected as classified; everything outside is treated as unclassified and is guaranteed to be so. Any connection between the inside and the outside, either physical or administrative, offers the potential for classified information transmission or manipulation.

There are three types of routes for possible, unintentional classified-information release across the IB.

(1) Some data pass through the IB in order for a monitor to receive useful information about a measured object. Although these data themselves are unclassified, care must be taken to ensure that classified information does not "leak" through this connection.

(2) All other connections (e.g., power supply) or operations (e.g., maintenance) that pass through the IB are also potential conduits for classified information transfer or manipulation. The connections can be addressed by hardware controls and the operations by access controls. However, the most straightforward way of minimizing the potential for classified data leakage or modification is to minimize the number of barrier crossings.

(3) Energy (e.g., acoustic, optical, radio-frequency) radiated from the inside to the outside of the IB could also carry classified information. Because there is no intentional transmission

across the barrier, the simplest solution is elimination of all transmission. This can involve a combination of hardware and access controls.

An effective AMS/IB will incorporate a suite of controls, both (1) administrative and access, and (2) hardware and software. As with many operations, the types of controls can be ordered as follows:

(1) elimination of the problem or transfer mode,
(2) substitution of another method to achieve the desired result,
(3) hardware or software elimination of the problem, and
(4) use of administrative or access control to eliminate the problem.

Thus, although administrative and access-control solutions to a problem are often the easiest, they are also the least reliable and should be considered only if no better method is available. They are perhaps most useful in combination with hardware and software solutions. People are fallible, especially in long-term operations; thus, any solution relying solely on people presents an opportunity for failure.

Although the IB "box" of Fig. 6 is conceptually useful for locating and minimizing vulnerabilities, this concept is overly simplistic and prone to single-point failure. A complete AMS/IB can incorporate a series of data-filtering stages followed by a final barrier to prevent the release of any classified information. The data filtering reduces the amount of classified information available throughout the detector system(s) and computers through proper choice of detection methods, hardware discriminator settings, data-processing methods, etc. Thus, the IB consists of several layers of protection rather than a single layer. The sum of all the layers ensures that no classified information is released. The multi-layer approach can provide the same amount of protection as a single layer, but without the single-point failure vulnerabilities inherent in a single-layer design. The end result is that no classified information is displayed in the open area.

Access to facilities where monitoring is carried out may involve restrictions on the materials that the monitors may bring into and remove from the facilities. The controls will also govern the activities permitted. Examples of such restrictions include: requirements for declaration of all items being brought in or requested for removal from the facility; examinations of all items declared; and physical-access restraints, including clothes changes and searches for undeclared items. In controlled-access locations within facilities, monitors will be under continuous supervision of facility security staff.

The host nation may determine that access controls and/or additional physical protection must be provided for any or all components of the AMS/IB. This may include items such as Non-Destructive Assay (NDA) instruments, computers, and connectors. Vaults, security guards, surveillance systems, locks, tamper-indicating seals, or similar devices can be used to guarantee that hardware and software have not been modified or tampered with in any way since last examined by all parties.

Additional protections can be provided administratively when implementation arrangements are developed for each specific facility. This may be accomplished with a detailed procedures rulebook specifying allowed behavior of monitors and facility operators during visits, routine maintenance, and at other times. An activity log may be maintained to provide continuity of knowledge.

Administrative controls may also be required in order to maintain operational security. Monitors may not be allowed to bring uncontrolled radiation detectors into the area. Uncontrolled detectors could include active devices (such as portable detectors brought in to check the response of the main system) as well as seemingly passive systems (such as film badges or other instruments that record personal dose or dose rate).

The implementation of the AMS/IB concept chosen for the FMTTD is illustrated in Fig. 7. In this figure, the data-barrier element in the data-output connection is explicitly called out. The data barrier is a simple (and hence easily validated) element residing on the IB whose only function is to ensure that no classified data are passed into the open area. An AMS/IB based on this concept can explicitly contain examples of many of the types of controls mentioned above. Many of the information filters, particularly those relating to detector choice, eliminate the possibility of transfer of unneeded classified data by eliminating any method of collecting those data. For example, hardware controls include data filters that limit the collection or transmission of classified data in hardware, (e.g., discriminator settings); software controls include programs designed to minimize the amount of data computed. The administrative and access-control elements of the IB also serve to prevent the release of classified information. Although only one layer of protection is shown, this represents multiple layers that have been implemented in the AMS/IB.

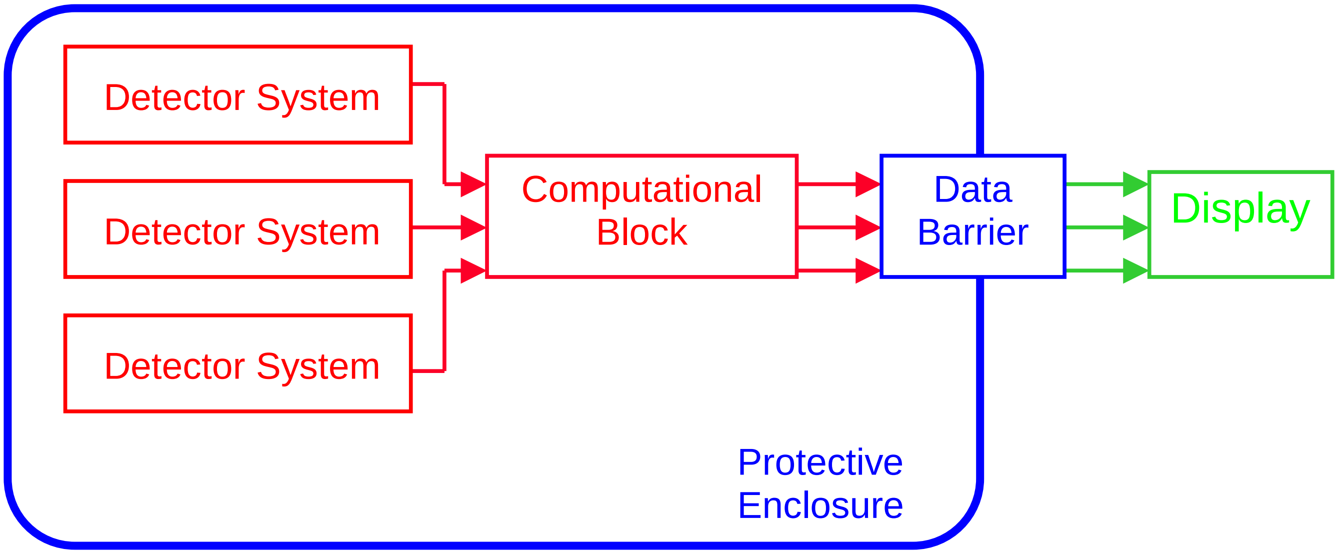

Fig. 7. Extension of the simple AMS/IB concept that was illustrated in Fig. 6. The attribute measurement detectors, the attribute-comparison computational block, and the data barrier are shown explicitly.

Authentication of the AMS/IB is important for acceptance of the system. Authentication is the process of demonstrating that the outputs from the system do, in fact, accurately reflect the contents of the objects presented to the system. Two methods of authentication (which might be used in concert) are (1) blind testing and (2) detector-system authentication. Although neither of these methods is ideal, a combination may produce acceptable results.

(1) A truly blind test would involve monitor presentation of an object, the contents of which were unknown to the host State. The correct identification of the contents would add confidence that the system was operating correctly. However, in reality, the State controls and must track the plutonium that would be used in this test object. Thus, a truly blind test may involve complex procedures or may not even be possible, depending on the material-accounting and physical-protection rules of the State.

(2) When no classified material or classified data are present, the monitor could test the operation of each stage of the detector system(s) using unclassified sources. In this case, complete output (spectra, multiplicities, shape, etc.) should be available to allow comparison with the attributes of the known reference object.

A combination of these techniques would involve on-site authentication of the unclassified reference materials using monitor-supplied equipment. Even though the host supplies the reference material, the monitoring party can draw totally independent conclusions as to what is in the reference material and how the AMS/IB should react.

4.0 ATTRIBUTES

An attribute measurement system determines whether a given object possesses, or fails to possess, certain “attributes” or characteristics. It does this by making direct measurements of several radiometric properties of the object. These quantities are then compared with agreed-upon, unclassified thresholds. The results of these comparisons determine the unclassified “attributes” of the object.

The six attributes that have been chosen for the Fissile Material Transparency Technology demonstration are:

(1) plutonium isotopic ratio,
(2) plutonium mass,
(3) absence of oxide,
(4) presence of plutonium,
(5) symmetry of the plutonium, and
(6) plutonium age.

These are six of the seven attributes that were discussed in previous technical exchanges among US and Russian experts. The seventh attribute discussed in those exchanges, namely presence of gallium, was dropped because it was not feasible to measure it.

Measurement of any of these attributes requires use of a detection system that generates classified data when used in conjunction with a classified object. Thus, an information barrier hides all of the “raw” data, and only unclassified yes/no threshold evaluations are displayed.

The thresholds used in the FMTTD have been discussed in previous technical exchanges. In some cases, they were selected for pragmatic reasons, solely for purposes of the demonstration. The following is a brief summary of the thresholds chosen.

> Presence of plutonium—Determined by looking for several characteristic plutonium gamma-ray peaks. The threshold is based on a statistical test at the five-sigma level.
>
> Plutonium isotopic ratio—As discussed in previous technical exchanges, the isotopic ratio threshold is whether the ratio of ^{240}Pu to ^{239} Pu is greater than, or less than, 0.1.
>
> Plutonium mass—The threshold is 500 grams. It is an unclassified fact that “all US weapon pits that contain plutonium contain at least 500 grams of plutonium, no elaboration.”
>
> Plutonium age—The threshold date between “old” and “new” is defined as 1 January 1997.
>
> Absence of oxide—The oxide attribute is based on two thresholds. Oxide is determined to be present ONLY IF alpha (a neutron multiplicity parameter) is greater than 0.5, AND the 871-keV gamma peak is present (at the three-sigma level). Otherwise, oxide is determined to be absent.
>
> Symmetry—As discussed in previous technical exchanges, the symmetry threshold is a 15% deviation, in any one of eight banks of detectors, from the mean neutron response averaged over all eight.

5.0 ATTRIBUTE MEASUREMENT SYSTEM WITH INFORMATION BARRIER

As shown in Fig. 8, the raw data generated in the detection systems pass into the shielded enclosure to the specific data acquisition systems and analyzers. Both the raw data from the detectors and the processed data from the analyzers will be classified if a classified item is being measured. The analyzed data pass into the computational block where the threshold values are stored and threshold comparisons are performed. The outputs from the computational block, in the form of yes/no data, are passed through the data barrier and to the unclassified display. Although the outputs from the computational block are unclassified, these signals are inside the shielded enclosure and are treated as possibly classified until they leave the enclosure through the data barrier.

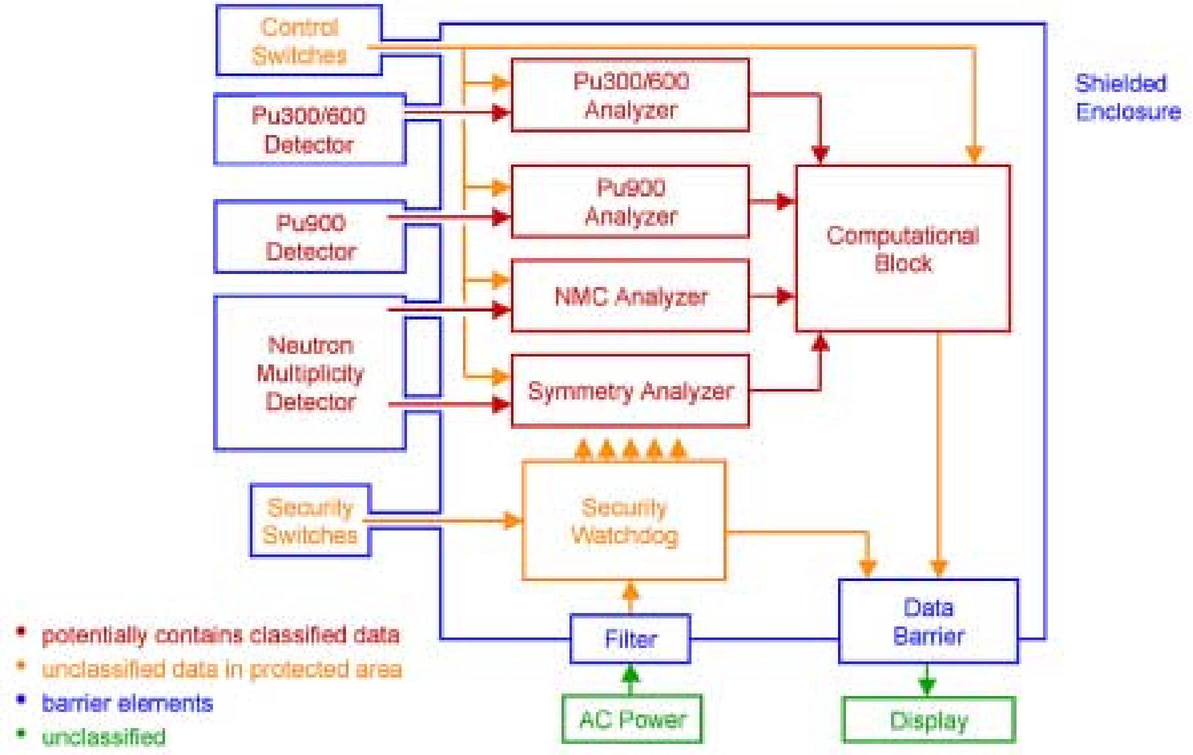

Fig. 8. Block diagram of the AMS/IB. Elements that may contain classified information are shown in red. Elements that are themselves unclassified but must be treated as classified because of their location or function are shown in orange. Unclassified elements are shown in green. The protective enclosure and associated elements are blue.

Several additional important elements of the AMS/IB are also illustrated in Fig. 8. All power for the AMS/IB enters the security watchdog through an AC line filter. The only function of the security watchdog is to monitor the security status of the entire system and to remove all power from all other AMS/IB elements if the access doors are opened or if classified material is introduced into the system incorrectly. The security mode of the security watchdog (and hence the entire AMS/IB) is set by the security switches. In addition, several data-control switches are used to start a background run, start calibration runs, and start measurement runs.

5.1 Detection Systems

As discussed above, the demonstration AMS/IB consists of three detector systems—a large HRGS, a medium-sized HRGS, and an NMC modified to provide access to the signals coming from individual banks of ^{3}He tubes. All three detector systems are collocated around a single measurement position within the NMC. Both HRGS detectors are aligned to “look” through the walls of the NMC at the source position.

Power to all electronic components housed in the shielded Electronics Rack (SER) and all detectors is controlled by the security watchdog. The filtered power cable leading to the security watchdog and all cables between the SER and all detectors are shielded.

5.1.1 Pu300/600—The aforementioned medium-sized germanium detector (50%) is used to supply the raw data for both the Pu300 and Pu600 analysis programs. These analysis programs run sequentially in a single computer so that, although Pu300 and Pu600 are separate analysis programs, they will both be running in a single HRGS system.

The Pu300 analysis uses the data from a region between 330 and 350 keV in the plutonium gamma-ray spectrum. This region includes spectral lines from ^{241}Am that can be used to determine the amount of americium present in the object and to infer the age of the plutonium in the object, because as plutonium ages, more and more ^{241}Am is created (in the plutonium) through β-decay of ^{241}Pu.

The spectral region from 630 to 670 keV is analyzed by the Pu600 code to provide both an isotopic ratio (^{240}Pu /^{239}Pu) for the object being measured and an indicator of the presence of plutonium. This spectral region includes lines from both ^{240}Pu and ^{239}Pu. A comparison of the strengths of these lines provides a measure of the isotopic ratio of the object, and the existence of the lines is indicative of the presence of plutonium.

The germanium detector for the Pu300/600 system is located in an interlocked solid enclosure that provides shielding and physical protection for the detector itself. The multichannel analyzer (MCA) and the analysis computer for this subsystem are located within the large shielded enclosure (the shielded electronics rack, or SER) together with all of the other AMS/IB electronics. The detector enclosure is connected to the shielded electronics rack by a set of shielded cables specific to the HRGS system.

5.1.2 Pu900—The larger (66%) germanium detector supplies raw data for the Pu900 analyzer. The Pu900 analyzer utilizes data from the region between 860 and 880 keV in the plutonium gamma-ray spectrum. This region includes lines indicative of ^{17}O content in the plutonium being measured. Thus, the Pu900 measurement is one test that may indicate the presence of oxides in the plutonium being measured.

The germanium detector for the Pu900 system is also located in an interlocked solid enclosure that provides shielding and physical protection for the detector itself. The MCA and analysis computer for this subsystem are located within the SER together with all of the other AMS/IB electronics. The detector enclosure is connected to the main shielded enclosure by a set of shielded cables specific to the HRGS system.

5.1.3 Neutron Multiplicity Counter—The NMC used in this demonstration consists of 32 ^{3}He tubes mounted within the four walls of a rectangular polyethylene enclosure. During normal operation, the count rates for noncoincident, doubly coincident, and triply coincident events (singles, doubles, and triples) are measured in the NMC detector. If the efficiency of this detector has been measured, then the singles, doubles, and triples can be used to calculate the ^{240}Pu-effective mass, the fraction of (α,n) reactions (or α), and the multiplication in the sample. Together with the isotopic ratio obtained from the Pu600 analyzer, the ^{240}Pu-effective mass is used within the computational block to calculate the Pu mass, and α is used as a second indicator of oxide presence, in addition to the output from the Pu900 analyzer. The final absence-of-oxide determination, requiring the presence of both indicators, is also made in the computational block.

The neutron detectors and polyethylene of the NMC are located in a solid metal enclosure that provides shielding and physical protection for the detector. The shift register and analysis computer for this subsystem are located within the SER together with all of the other AMS/IB electronics. The detector enclosure is connected to the SER by a set of shielded cables specific to the NMC system. This bundle of shielded cables is located within an electrical conduit.

5.1.4 Symmetry Detector**—**As well as being combined for the multiplicity measurement described in section 5.1.3, signals from the eight octants of the neutron detector are counted individually to provide an indication of the axial symmetry of the tested object.

As described above, the neutron detectors are located in a solid metal enclosure. The analysis computer is located in the SER. The detector enclosure is connected to the SER by a set of shielded cables specific to the symmetry system, which is also located within an electrical conduit.

5.2 Analyzers

All of the CPUs used in the AMS/IB are small and easily inspectable, with documented functionality. Each of the four measurement systems discussed in section 5.1 includes a separate CPU as its analyzer. Among other advantages, dedication of these functions to separate CPUs allows each measurement system to be tested separately without requiring the remainder of the AMS/IB to be operational.

The analyzer CPUs are all implementations of the PC/104 standard, and all use DOS operating systems. The software is stored in ROM, memory which cannot be modified or erased. The CPU boards are commercially available; for this demonstration, the commercial boards are used with their original excess functionality disabled but not removed. All of the analyzers are located within the SER and all receive their power from the security watchdog.

5.3 Computational Block

The attribute threshold values are stored in the computational block in read-only memory, and attribute threshold comparisons are also performed in this element. In addition, any calculations requiring the results from more than one analyzer are performed in the computational block. There is no interconnection between analysis computers aside from the computational block. The inputs to the computational block from the analyzers are potentially classified but the outputs from the computational block to the data barrier are unclassified (yes/no) values.

As implemented in this demonstration, the computational block uses a small, easily inspected computer with limited hardware and software functionality. The demonstrated computational block is based on an Ampro 3SXI 386 computer with an Emerald digital I/O card. This PC/104 specification CPU runs a DOS operating system. As with the analysis CPUs, there is no data connection between the security watchdog and the computational block.

5.4 Data Barrier

The only function of the data barrier is to pass unclassified information in one direction, from inside the SER to the display. Operationally, this can be separated into two requirements.

(1) The data barrier passes information from the computational block to the display—no information may be passed from the display to the remainder of the system.
(2) The data barrier may not allow classified information to pass through itself.

In ordinary operation, no classified information is presented to the data barrier by the computational block. In any event, the data barrier is constructed from simple hardware so that it cannot be “reprogrammed” to pass other types of information.

As implemented in the demonstration system, the data barrier utilizes fiber optics drivers and fiber optic links to the display to ensure that no data can pass back into the SER. The fiber optic links also ensure that no extraneous electrical signals can be picked up or radiated by the links to the display. The fiber optics drivers are driven by either flip-flops or low-pass filters. The flip-flops are clocked once each measurement cycle so that only one change of output state is allowed for each measurement. Ideally, all signals derived from the computational block would pass through flip-flops clocked by the security watchdog. However, in this implementation, all of the threshold data signs do pass through flip flops, but the “measurement complete” and “error” signals pass through low-pass filters. In this demonstration system, the flip-flops are clocked by the computational block. The two security signals are derived directly from the security watchdog.

5.5 Display

The unclassified display is another simple hardware circuit with no computer-controlled functions. The optical signals transmitted by the data barrier are received in optical receivers. The optical receivers in turn are connected to LED drivers, which are connected directly to the red and green LEDs. All power for the display is DC and is generated within the shielded enclosure and sent to the display through a shielded cable. Thus, the security watchdog also controls the power to the display.

The display for the FMTTD AMS/IB has eight red and eight green LEDs. Six pair of LEDs are used to indicate passing or failing the six attribute tests. The remaining two pair of LEDs are for system “housekeeping” functions. One pair indicates the security status of the AMS/IB (whether the system is open [red] or secure [green]). An additional green LED indicates that a measurement has been completed and the final red LED is indicative of a malfunction within the AMS/IB.

5.6 Security Watchdog

The demonstration AMS/IB can operate with the access doors open or closed. When the access doors are closed, the red and green display is the only output from the system. In this configuration, either classified items or unclassified reference materials can be measured, but only the simple unclassified display is available for data output. Whenever the access door is opened, all power is immediately removed from the system. This, in addition to an active purge procedure, will ensure that no classified information can remain in the AMS/IB after the door is opened. If, and only if, a modified container (containing no classified material) is present in the NMC, will the security watchdog restore power to the AMS/IB following a delay of approximately 20 seconds. This allows authentication measurements to take place using unclassified reference materials. If the modified container is removed from the AMS/IB while the door is open, all power to the system is immediately cut off and remains off.

In addition, the security watchdog incorporates a SCRAM switch that, if pressed, removes all power from the AMS/IB regardless of whether or not classified material is present.

5.6.1 Active Purge—Any time the doors are opened, all power is removed from the system. Because no data are written into nonvolatile memory during AMS/IB operation, this operation is intended to remove all classified information. (This power-down event is termed a “passive purge.”) However, if a passive purge is considered not sufficient, the volatile memory may be overwritten before the purge is considered complete. (This overwriting method is termed an “active purge.”)

An active purge of the memory in the demonstration AMS/IB can be performed procedurally rather than electronically using the following procedure:

(1) the SCRAM button is pressed and manually released before opening the access door; and

(2) **before** the door is opened, the computers are allowed to restart (which overwrites their entire RAM).

This procedure can be repeated as many times as required to achieve appropriate sanitization of the system.

5.7 Switches

The demonstration AMS/IB incorporates two types of switches. (1) The security functions of the security watchdog are controlled by the SCRAM switch, the door switches, and the security switches themselves. All switches performing security functions operate in a “fail-safe” configuration, i.e., if any cable connecting any of these switches is not connected fully, then the switch is assumed to be open. (2) The data-analysis systems are controlled by the data-control switches, a set of mechanical switches separate from the security functions. If the cables to the data switches are not connected correctly, no measurements can be initiated and the system will not function until the connection is fixed.

A key feature of the demonstration AMS/IB is the separation between the security and data switches. The security switches control the security watchdog (and only the security watchdog) directly. The security watchdog, in turn, controls the power to all of the other elements of the AMS/IB. There is no other connection between the security watchdog and the CPUs. Thus, the CPUs do not “know” the position of the security switches and have no way of “knowing” whether they are processing classified or unclassified data. This adds assurance that the analyzers will operate similarly with classified items and unclassified items.

Similarly, the data switches are demonstrably not connected to the security watchdog. No manipulation of the data switches can change the security status of the system.

5.7.1 Data-Control Switches—These push-button switches, operated by the material handler (as opposed to a monitor or observer) control the starting of background, calibration, or measurement cycles within the AMS/IB (Fig. 9). Once any type of cycle has been started, additional switch closures have no further effect. These switches are simple hardware closures – no further electronics or processing capability is included in this part of the AMS/IB. There is never any classified data in the control box nor the shielded cables that connect it to the SER.

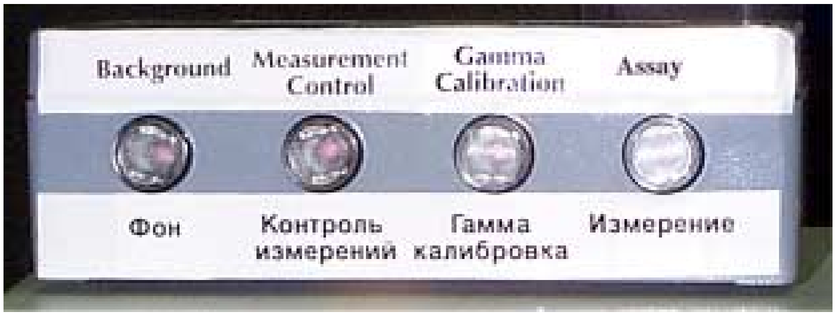

Fig. 9. The data-control switches for the AMS/IB.

Ideally, the source container itself would make the determination as to what type of measurement were required and the handler would push a single “start” switch. However, for this demonstration, the handler will also make a determination as to which measurement type is appropriate.

5.7.2 Security Switches—A container that holds a classified item presses against all of the mechanical security switches when the container is placed in the NMC. Thus, the system assumes that every container contains classified material unless that container has been specifically modified so as not to contact two of the security switches. The cables that transmit the switch configuration to the security watchdog are enclosed in a shielded conduit.

In the demonstration AMS/IB, the security switch consists of four switches in series, any one of which is sufficient to indicate a classified container. Two of these switches (normally closed) open if any container, other than the specially modified one, is placed in the NMC. The other two (normally open) switches are closed when any container (modified or otherwise) is placed in the NMC. The AMS/IB can only be operated with the door open if all four switches are closed, indicating that a specially modified container has been inserted.

5.7.3 Door Switches—The doors to the SER and the doors to the HRGS detectors are equipped with interlock switches. Each door of the SER has two switches (top and bottom), and each door of the HRGS detector enclosures has one switch. All six of these door switches are connected in series.

All of these switches must be closed (i.e., all doors must be closed) before classified material can be measured in the AMS/IB.

5.7.4 SCRAM Switch—In addition to the door switches, a SCRAM switch is mounted on the shielded enclosure. The SCRAM switch is operable from outside of the SER. If the SCRAM switch is pressed, all power is immediately removed from the AMS/IB (other than from the security watchdog itself) regardless of the position of the other security switches. The AMS/IB cannot be restarted until the SCRAM switch is manually reset.

As detailed in section 5.6, the SCRAM switch also forms part of the active-purging operation in the demonstration AMS/IB.

6.0 THE DEMONSTRATION

The objectives of the FMTTD are:

(1) to demonstrate to the Russian delegation that an attribute measurement system with information barrier (AMS/IB) can be built with sufficient protection to allow measurement of classified components without revealing classified information, and

(2) to construct this AMS/IB in such a manner as to convince the Russian delegation that it would be possible for an inspecting party to fully authenticate operation of the system.

The demonstration will take place in the Los Alamos National Laboratory Technical Area-18 “High Bay” facility, where special arrangements have been made to accommodate the AMS/IB equipment and the large number of visitors who will be present. Special security procedures will be implemented, including most notably a requirement for all participants (Russian and American) to change clothes and shoes before entering the High Bay. No personal or hand-held articles, except eyeglasses, will be permitted into the High Bay, and each participant will be carefully screened for prohibited articles.

The demonstration will consist of the following main steps:

(1) AMS/IB startup—After arrival of the first Russian visitors, the attribute measurement system will be started.
(2) Background and energy calibrations—Background and energy calibrations will be performed and a measurement-control procedure for the NMC will be carried out.
(3) Authentication measurements—Two unclassified sources will be measured in the AMS/IB to show the correct operation of the system. The first source will be an asymmetric array of plutonium plates. The second will be a 1.5-kilogram plutonium oxide sample. One of these will also be measured with another, independent, gamma-spectroscopy system to confirm the characteristics of the source.
(4) Nuclear weapon component—The AMS/IB will be placed in secure mode, and the nuclear weapon component will be measured.
(5) Remeasurement—One of the authentication sources will be remeasured, this time in secure mode, to show consistency of the attribute response.
(6) Security watchdog function—The security watchdog function will be demonstrated, showing that the system shuts down if any attempt is made to breach the information barrier.
(7) Shutdown and secure AMS/IB—The system will be shutdown.
(8) Equipment viewing—The Russian visitors will be invited to approach the equipment for closer examination and for detailed discussions with technical experts.
(9) Authentication case study (to be completed the next day)—Authentication concepts and approaches will be illustrated, using the computational block as an example.

7.0 THE IMPORTANCE OF COOPERATIVE DEVELOPMENT

The FMTTD is intended as a proof of concept. The goals are to establish that the six selected attributes can be measured while protecting classified information and that it would be possible, through a series of authentication measures, to instill confidence that the system operates as it should.

Full implementation of such a system is a more difficult task. What is straightforward in concept may become very complex when all the details of a particular application are considered. Furthermore, a design choice that works well enough for proof of concept in an R&D laboratory may be far from optimal in an industrial setting. And finally, what works in the US may require adaptation to work as well in Russia, and vice versa. The security requirements are not identical, the operating conditions are not the same, and the technical environment is different.

If both countries are to have complete confidence in concrete applications of a technology such as the AMS/IB, a one-week technical exchange to demonstrate the equipment and concepts is not sufficient. Only through a well-planned, cooperative development effort and cooperative implementation will it be possible to fully satisfy the requirements of both sides.

The CTR program is prepared to immediately initiate a joint development effort and will provide separately a draft statement of work for the system needed for the FMSF Absolute Control Room. A cooperative planning effort should be initiated to begin this process. Among the tasks that could be included in the plan are:

- definition of Russian requirements for an AMS/IB;
- identification of Russian technologies to perform required attribute measurements;
- refinement of the information barrier architecture to meet Russian requirements;
- development and implementation of mutually acceptable authentication techniques;
- optimization of equipment;
- development of software;
- cooperative work on methods of ensuring reliability and maintainability; and
- development of operating procedures.

Implementation of the cooperative plan will require strong management on both sides and close coordination of the work. Because of the importance of this technology, the Cooperative Threat Reduction program has assigned a very high priority to this effort and is prepared to fully fund an ambitious cooperative development program.